PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-282155
(43)Date of publication of application : 31.10.1997

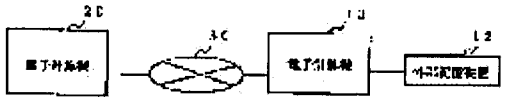
(51)Int.Cl. G06F 9/06
G06F 12/14
G09C 1/00
G09C 1/00
H04L 9/10
H04L 9/32

(21)Application number : 08-088635
(22)Date of filing : 10.04.1996

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : HAYASHI SEIICHIRO
MURATA YUICHI

(54) METHOD FOR EQUIPPING CIPHER AUTHENTICATION FUNCTION

(57)Abstract:
PROBLEM TO BE SOLVED: To safely realize a conventionally provided security function by making the unauthorized decoding and alteration, etc., of a cipher authentication program impossible.
SOLUTION: In an external storage device 12, the cipher authentication program and authentication information ciphered or to which a digital signature us attached are stored. At the time of execution, an electronic computer 10 loads the cipher authentication program and the authentication information of the external storage device 12 to its own storage part, decodes them and verifies the propriety of the decoded cipher authentication program itself. By the program guaranteed to be proper, the electronic computer 10 ciphers a document and multi-media information, generates the digital signature, executes cipher communication and signature communication, etc., with the other electronic computer 20 and clears the cipher authentication program and the authentication information of its own storage part when the execution is ended.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平9－282155

(43)公開日　平成９年(1997)10月31日

(51)Int.Cl.[6]		識別記号	庁内整理番号	Ｆ Ｉ			技術表示箇所
Ｇ０６Ｆ	9/06	５５０		Ｇ０６Ｆ	9/06	５５０Ａ	
						５５０Ｄ	Ｃ４
						５５０Ｚ	
	12/14	３１０			12/14	３１０Ｚ	
Ｇ０９Ｃ	1/00	６３０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６３０Ｚ	

審査請求　未請求　請求項の数４　ＯＬ　（全 ５ 頁）　最終頁に続く

(21)出願番号　特願平8－88635

(22)出願日　平成８年(1996)４月10日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　林　誠一郎
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　村田　祐一
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

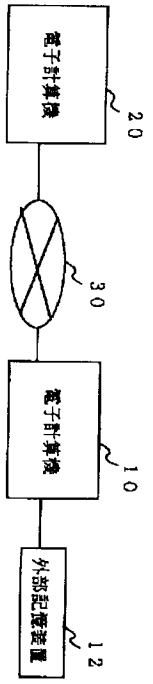
(74)代理人　弁理士　鈴木　誠

(54)【発明の名称】　暗号認証機能の装備方法

(57)【要約】

【課題】　暗号認証プログラムの不正な解読や改ざん等を不可能とし、本来有するセキュリティ機能を安全に実現する。

【解決手段】　外部記憶装置１２に、暗号化またはディジタル署名を付した暗号認証プログラムと認証情報を格納しておく。電子計算機１０は、実行時、該外部記憶装置１２の暗号認証プログラムと認証情報を自記憶部にロードし、復号化し、該復号化した暗号認証プログラム自体の正当性を検証する。電子計算機１０は、正当であることを保証されたプログラムにより、文書やマルチメディア情報を暗号化したり、ディジタル署名を生成して、他の電子計算機２０との間で暗号通信、署名通信等を実行し、該実行を終了したなら自記憶部の暗号認証プログラムと認証情報をクリアする。



1

【特許請求の範囲】

【請求項１】　可搬型の記憶媒体に、暗号化またはディジタル署名を付した情報セキュリティ機能を有する暗号認証プログラムと認証情報を格納し、前記記憶媒体の暗号認証プログラムと認証情報を電子計算機にロードして復号化またはディジタル署名検証して使用し、該使用後は電子計算機内の暗号認証プログラムと認証情報をクリアすることを特徴とする暗号認証機能の装備方法。

【請求項２】　請求項１記載の暗号認証機能の装備方法において、暗号認証プログラムとして、暗号化プログラムと暗号鍵作成プログラムと秘密暗号鍵方式によって暗号化されたディジタル署名生成・検証プログラム、及び、秘密暗号鍵方式によって暗号化された認証情報を記憶媒体に格納し、電子計算機からの指示により、前記暗号認証プログラム及び認証情報を記憶媒体から電子計算機にロードし、前記暗号鍵作成プログラムにより暗号鍵を作成し、該作成した暗号鍵と前記暗号化プログラムにより、前記暗号化されたディジタル署名生成・検証プログラム、認証情報を復号化することを特徴とする暗号認証機能の装備方法。

【請求項３】　請求項１記載の暗号認証機能の装備方法において、暗号認証プログラムとして、暗号化・復号化機能と暗号鍵作成機能を含む暗号認証制御プログラムと、秘密暗号鍵方式によって暗号化された、暗号化プログラムとディジタル署名生成・検証プログラム、及び、秘密暗号鍵方式によって暗号化された認証情報を記憶媒体に格納し、電子計算機からの指示により、前記暗号認証プログラムと認証情報を記憶媒体から電子計算機にロードし、前記暗号認証制御プログラムの暗号鍵作成機能により暗号鍵を作成し、該作成した暗号鍵により、前記暗号認証制御プログラムの暗号化・復号化機能を用いて、前記暗号化された暗号化プログラムとディジタル署名生成・検証プログラムと認証情報を復号化することを特徴とする暗号認証機能の装備方法。

【請求項４】　請求項１記載の暗号認証機能の装備方法において、暗号認証プログラムと認証情報に公開鍵暗号鍵方式によってディジタル署名を生成し、前記暗号認証プログラムと認証情報とそのディジタル署名を記憶媒体に格納し、電子計算機からの指示により前記暗号認証プログラムと認証情報そのディジタル署名を記憶媒体から電子計算機にロードし、暗号認証プログラムのディジタル署名生成・検証プログラムにより、暗号認証プログラムと認証情報の署名を検証することを特徴とする暗号認証機能の装備方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、複数の電子計算機間で暗号署名通信を行うシステムにおいて、暗号認証機能を有するセキュリティプログラムの電子計算機内での装備方法に関する。

2

【０００２】

【従来の技術】従来、セキュリティ機能を有する暗号認証プログラムである暗号化プログラムやディジタル署名プログラムは、外部記憶装置や電子計算機内にそのままの形で格納されており、実行時にパスワード等により操作者を認証し、許可された操作者が暗号認証プログラムを走行させる方法をとっていた。

【０００３】

【発明が解決しようとする課題】暗号認証プログラムは、情報の隠匿や改ざん防止等のセキュリティ機能を果すプログラムである。この暗号認証プログラムを記憶媒体上で暗号化やディジタル署名されずに格納されていると、誰もがプログラムを解読して、そのプログラムを都合のよい様に改ざんして実行させることが容易に行える。このため、暗号認証プログラムの本来のセキュリティ機能が果たせなくなるという問題がある。

【０００４】本発明の目的は、記憶装置や電子計算機に格納される暗号認証プログラムの不正な解読や改ざんや不正なプログラムの置き換えを不可能とし、本来有するセキュリティ機能を安全に実現することにある。

【０００５】

【課題を解決するための手段】本発明は、暗号認証プログラムと認証情報を暗号化またはディジタル署名を付けて、可搬型の記憶媒体に格納し、実行時に電子計算機にロードして復号化し、暗号認証プログラム自体の正当性を検証する。これにより、不正者が例え記憶媒体を手に入れたとしても、格納されている暗号認証プログラムを解読したり、改ざんしたりすることができないようになる。また、暗号認証プログラムの実行後は、電子計算機にロードされた暗号認証プログラムや認証情報はクリアし、電子計算機内の記憶部にそのままの形で残らないようにする。

【０００６】

【発明の実施の形態】以下、本発明の一実施例について図面により説明する。図１は本発明が適用される通信システムの概略構成である。図において、電子計算機１０、２０はネットワーク３０で接続されている。電子計算機１０は可搬型の外部記憶装置（記憶媒体）１２を有する。該外部記憶装置１２に、暗号認証プログラムと認証情報を暗号化またはディジタル署名を付して格納しておく。電子計算機１０は、実行時、外部記憶装置１２の暗号認証プログラムと認証情報をロードして復号化、ディジタル署名検証した後、該プログラムにより、文書やマルチメディア情報を暗号化して、電子計算機２０との間で暗号通信、署名通信等を実行する。そして、実行後は、電子計算機１０の暗号認証プログラムと認証情報をクリアする。

【０００７】図２は、本発明の処理手順のフローチャート例、図３及び図４は外部記憶装置に格納されるプログラムの構成例である。以下、図１、図２、図３、図４に

より、本発明の実施例を説明する。

【０００８】〈実施例１〉これは、暗号認証プログラムを図３に示す構成とする実施例である。

ステップ１：外部記憶装置へのプログラム、認証情報の格納

図３の暗号認証プログラム３００に対して、プログラムの開発者や供給者等のディジタル署名を図２の処理２０１により生成する。認証情報３１０については、操作者を認証する認証者がディジタル署名する。さらに、暗号化プログラム３００中の暗号鍵生成プログラム３０１と暗号化プログラム３０２を除き、改ざんを回避すべく、署名生成・検証プログラム３０３及び認証情報３１０をあらかじめ操作者のパスワードから作成された暗号鍵を使い処理２０２により暗号化し、図１の外部記憶装置（記憶媒体）１２に処理２０３により格納する。外部記憶装置１２としては、ＰＣＭＣＩＡインタフェースを有するＰＣカードやフロッピィディスク等が考えられる。

【０００９】ステップ２：プログラムのロードと復号化

外部記憶装置１２に格納された、暗号鍵生成プログラム３０１、暗号化プログラム３０２、署名生成・検証プログラム３０３からなる暗号認証プログラム３００、及び、認証情報３１０を電子計算機１０へ処理３０４によりロードする。外部記憶装置１２の所有者はパスワード（暗号認証プログラムの暗号化に使用した暗号鍵作成に使ったパスワード）を処理２０５により入力し、暗号鍵生成プログラム３０１によりは該パスワードを基に暗号鍵を処理２０６により作成する。上記作成した暗号鍵により、暗号化されている署名生成・検証プログラム３０３と認証情報３１０を処理２０７により復号化する。

【００１０】ステップ３：ロードプログラムの署名検証

ディジタル署名した暗号認証プログラム３００と認証情報３１０について、署名生成・検索プログラム３０３に用いたプログラムの開発者や供給者等の秘密鍵に対応する公開鍵で署名検証し、改ざんされていない正当なプログラムであることを処理２０８より検証する。

【００１１】ステップ４：暗号認証機能の実行

正当であることを保証されたプログラムにより、文書やマルチメディア情報を暗号化したり、ディジタル署名を生成して、ネットワーク３０を介した他の電子計算機２０との間で暗号通信、署名通信を処理２０９により実行する。暗号通信、署名通信等の実行を終了した後、電子計算機１０の記憶部にロードした暗号認証プログラム３００と認証情報３１０を処理２１０によりクリアする。

【００１２】〈実施例２〉これは、暗号認証プログラムを図４に示す構成とする実施例である。

ステップ１：外部記憶装置へのプログラム、認証情報の格納

暗号認証プログラム４００中に、暗号化・復号化機能と暗号鍵作成機能を持った暗号認証制御プログラム４０１を加える。実施例１と同様に、暗号認証プログラム４００に対して、ディジタル署名を処理２０１により生成する。さらに、暗号認証プログラム４００中の暗号認証制御プログラム４０１を除く暗号化プログラム４０２と署名生成・検索プログラム４０３及び認証情報４１０をあらかじめ操作者のパスワードから作成された暗号鍵を使い処理２０２により暗号化し、外部記憶装置１２に処理２０３により格納する。

【００１３】ステップ２：プログラムのロードと復号化

外部記憶装置１２に格納された暗号認証プログラム４００と認証情報４１０を電子計算機１０へ処理２０４によりロードする。外部記憶装置１２の所有者はパスワード（暗号認証プログラムの暗号化に使用した暗号鍵作成に使ったパスワード）を処理２０５により入力し、暗号認証制御プログラム４０１の鍵生成機能によりパスワードを基に暗号鍵を処理２０６により作成する。上記作成した暗号鍵により、暗号認証制御プログラム４０１の復号化機能を用いて、暗号化されている暗号認証プログラム４００中の暗号化プログラム４０２と署名生成・検証プログラム４０３及び認証情報４１０を処理２０７により復号化する。

【００１４】ステップ３：ロードプログラムの署名検証

実施例１と同様であるので省略する。

【００１５】ステップ４：暗号認証機能の実行

実施例１と同様であるので省略する。

【００１６】以上、二つの実施例を説明したが、暗号認証プログラムと認証情報に、公開鍵暗号方式によってディジタル署名を生成し、暗号認証プログラムと認証情報とそのディジタル署名を記憶媒体に格納することでもよい。この場合、暗号認証プログラムと認証情報とそのディジタル署名を記憶媒体から電子計算機にロードしたなら、暗号認証プログラムのディジタル署名生成・検証プログラムにより、暗号認証プログラムと認証情報の署名を検証して、正当であることを保証する。

【００１７】

【発明の効果】本発明では、暗号認証プログラムとその関連情報を暗号化またはディジタル署名を付けて、可搬型の記憶装置もしくは媒体に格納し、実行時に暗号認証プログラム自体の正当性を検証可能にしたことにより、暗号認証プログラムの不正な解読や改ざんや不正なプログラムの置き換えが不可能となり、本来有するセキュリティ機能を易全に実現することが可能になる。

【図面の簡単な説明】

【図１】本発明が適用される暗号通信署名システムの概略構成図である。

【図２】本発明の一実施例の処理フローチャートである。

【図３】本発明の実施例１を説明するプログラムの構成例である。

【図４】本発明の実施例２を説明するプログラムの構成例である。

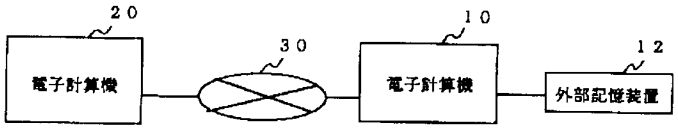
5

【符号の説明】
１０，２０　電子計算機
１２　外部記憶装置（記憶媒体）
３００，４００　暗号認証プログラム
３０１　暗号鍵作成プログラム

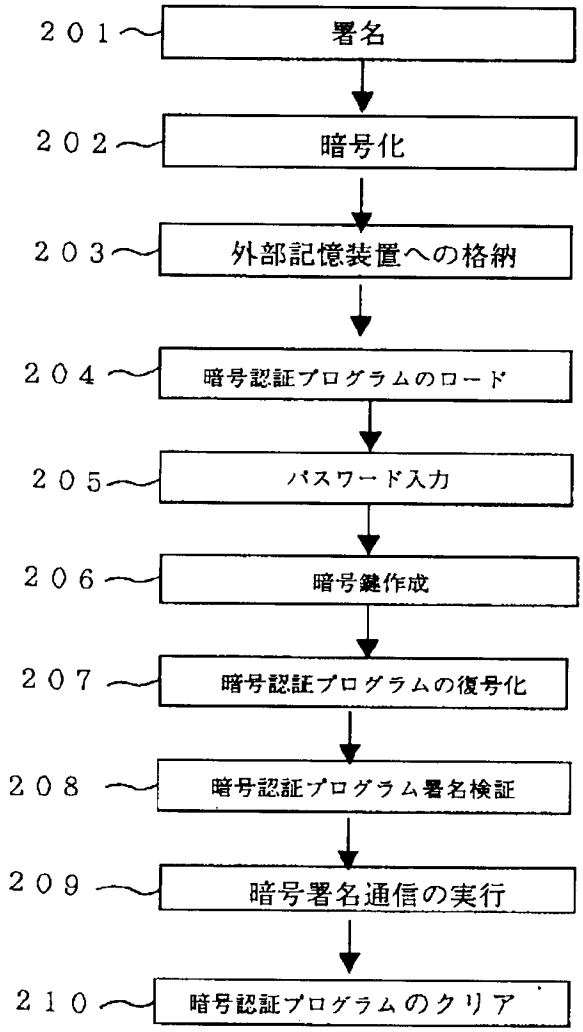
6

＊３０２，４０２　暗号化プログラム
３０３，４０３　署名生成・検証プログラム
３１０，４１０　認証情報
４０１　暗号認証制御プログラム
＊

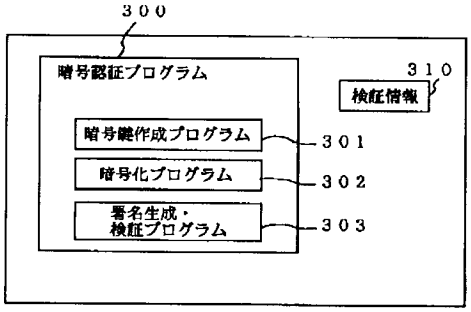
【図１】



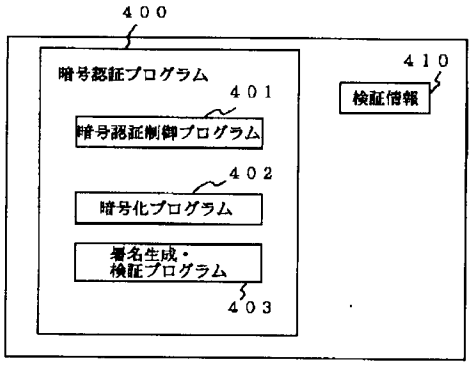
【図２】



【図３】



【図４】



フロントページの続き

(51)Int.Cl.[6]		識別記号	庁内整理番号	FI		技術表示箇所
Ｇ０９Ｃ	1/00	６４０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６４０Ｚ
Ｈ０４Ｌ	9/10			Ｈ０４Ｌ	9/00	６２１Ｚ
	9/32					６７５Ｚ